data) used to perform one or more sub-operations (which can be, for example, one or more mathematical primitive operations); ii) a second set of code, distinct from the first set of code, used to perform one or more cryptographic operations, the second set of code including one or more instructions that cause performance of instructions and/or use of data from the first set of code so that the one or more sub-operations are performed; and iii) a third set of code for allowing and mediating access to the first set of code from a device external to a device of which the computer readable storage medium is part. The computer readable storage medium can be a data storage device or devices that, together with a processor, can be embodied in a cryptographic device to flexibly provide cryptographic operations in the cryptographic device.

Please replace the paragraph beginning at page 5, line 13, with the following rewritten paragraph:

This embodiment of the invention enables easy and secure modification (expansion, reduction or changing) of application code via the exposure of, for example, the mathematical primitive operations available on a particular cryptographic device. In particular, this embodiment of the invention enables modification of available cryptographic operations at a relatively high level of programming abstraction, thus enabling such modification to be accomplished relatively easily. Further, this embodiment of the invention enables the modification to be accomplished in

a manner that does not necessitate or allow access by the application developer to other operations of the cryptographic device, thus providing security for the proprietary code and/or cryptographic keys of other persons or entities that may be present on the cryptographic device. Additionally, this embodiment of the invention can allow storage of a part of the code for the cryptographic operations that need never change in a small and unmodifiable storage device (ROM), while a part of the code of the cryptographic operations that it may desired to change is stored in a larger and modifiable storage device (EEPROM), thus retaining the capability of modifying the cryptographic operations present on a cryptographic device, while minimizing or eliminating any limitation on the number and/or complexity of the cryptographic operations that can be provided in the cryptographic device.

Please replace the paragraph beginning at page 8, line 2, with the following rewritten paragraph:

FIG. 4 is a block diagram of the functional components of a cryptographic device 400 according to an embodiment of the invention. The block 401 (hereinafter sometimes referred to as "the mathematical primitives storage area") represents instructions and/or data ("code") that enables the performance of one or more mathematical primitive operations. The block 402 (hereinafter sometimes referred to as "the cryptographic operations storage area") represents code that enables the performance of one or more

cryptographic operations. In general, the block 402 does not include code that enables the performance of mathematical primitive operations. The block 403 (hereinafter sometimes referred to as "the cryptographic characteristic table") represents data ("access permission data") that specifies cryptographic characteristics in accordance with which one or more of the mathematical primitive operations or cryptographic operations are performed. The block 404 represents code (hereinafter sometimes referred to as "the access allowance verifier") that, using the access permission data, controls access by a user to the mathematical primitive operations and cryptographic operations. Finally, the block 405 represents code (hereinafter sometimes referred to as "the key manager") for storing and accessing cryptographic keys and certificates.

Please replace the paragraph beginning at page 8, line 26, with the following rewritten paragraph:

In general, requests by application code 406 for performance of cryptographic operations are received by the access allowance verifier 404 from the application code interface 407. Each request is evaluated by the access allowance verifier 404 to ensure that the request is allowable. Whether a request is allowable is evaluated by comparing the cryptographic characteristics associated with the request to the availability of such cryptographic characteristics, as indicated by the access permission data

stored in the cryptographic characteristic table 403. If the request is allowable, then cryptographic operations are performed in accordance with the request, as described further below.

Please replace the paragraph beginning at page 10, line 10, with the following rewritten paragraph:

Preferably, the access permission data of the cryptographic characteristic table 403 are stored in a programmable read-only memory (PROM). The use of such a data storage device enables flexibility in establishing the access permission data (i.e., the availability of cryptographic characteristics) of a cryptographic device, since the access permission data can be established at device fulfillment (see FIG. 1). Thus, a single mass-produced type of cryptographic device can be tailored to meet cryptographic needs for many different applications. Further, the use of such a data storage device enables permanency - and, therefore, security - in establishing the access permission data of a cryptographic device, since once the access permission data are established, the access permission data cannot be changed. Thus, a single mass-produced type of cryptographic device can be tailored to satisfy domestic demand for robust cryptographic capabilities or to conform to export regulations dictating somewhat less robust cryptographic capabilities, while, in the latter case, providing confidence that the limitations

on the cryptographic capabilities cannot be circumvented once the cryptographic device has been exported to a user.

Please replace the paragraph beginning at page 16, line 13, with the following rewritten paragraph:

The cryptographic operations storage area 402 can include any desired cryptographic operations. For example, the cryptographic operations included in the cryptographic operations storage area 402 can include, but are not limited to, the following operations: RSA encrypt, RSA decrypt, DSA sign, DSA verify, 3-key triple DES, Diffie-Hellman and elliptic curve. However, it is emphasized that any other cryptographic operations, including, in particular, cryptographic operations that are developed in the future, can be included in the cryptographic operations storage area 402. It is an important aspect of the invention that any cryptographic operation can be easily implemented in a cryptographic device according to the invention.

IN THE DRAWINGS

Applicants request permission to amend FIG. 4 as indicated in red on a copy of FIG. 4 as originally filed that is enclosed with this Response.